Analysis of Alternatives for a Security Information and Event Management Tool in a Virtualized Environment

By: Roy A Sepulveda Rodriguez
Dr. Nelliud Torres Batista
Polytechnic University of Puerto Rico

Abstract

Security Information and Event Management is a software tool that increases the cyber situational awareness of a system. Since many products are available in the market, there is a desire from companies and individuals to establish which candidate is the correct for their necessities. This project dives into why it is necessary, and recommended for an enterprise to deploy such a tool. It will produce a list of quantifiable metrics in which needs can be leveraged against. It also intends to present a sample attack methodology to test the desired product. To further explain the relation between metrics and needs, example user cases are generated to provide a satisfactory solution. It is intended for the interested party to understand all vectors that relate to the acquisition of a product, and by using the conclusions presented, reach a decision, or accelerate their selection process.

Background

A Security Information and Event Management tool is a software product that monitors a computing system for cyber security violations in a real time manner. It fulfills this task by doing the following services, log management, IT regulatory compliance event correlation, endpoint protection and in some cases countermeasure response. It can parse and correlate log information into human readable events. Events are triggered when some security rule is being infringed, and it will display some type of alert. This type of functionality is often referred to as situational awareness.

This tasking is often facilitated by the use of a graphical user interface, which allows a user to see these events in real time, then making it possible to mitigate a possible attack in progress, or look at existing data to perform forensic studies to discover vulnerability vectors or patterns in a series of events. There are many open source and commercial SIEM tools available, and it could prove difficult to choose the correct tool that will satisfy the interested parties need.

Motivation and Problem Statement

As a member of the Cybersecurity Workforce it is imperative that I provide my customers with tools and solutions to help them complete their mission while keeping their systems as safe as possible. To reach a decision on which product to choose, the person or group needs to understand all the effects the acquisition will bring to the interested party. To answer all these questions a process called analysis of alternatives (AoA) is performed. An analysis of alternatives is a process used to determine which solution to a problem is more beneficial than its peers based on empirical data and evaluation. The following are Several factors play a role in this AoA.

- What are the measurable cybersecurity benefits of implementing a SIEM in an enterprise network?
- How well do SIEM tools comply with industry standardized security requirements?
- Does the SIEM implementation actually provide the system with all the purported functions it offers?
- What evaluation metrics and methodologies can be implemented to properly compare alternative SIEM tools?
- How will they fare against each other based on data?

Methodology

This research will employ quantitative and qualitative methodologies. Industry standards will be used to establish different framework objects. Ones for a summary of compliance to compare which product meets more requirements. Another that will apply numeric values to found criteria, to establish which has the "most" points. Qualitative approach can be seen in areas where the human experience, such as looking at the product, or handling it, while some numeric values can also be applied to it, it is inferred that the expected value will be more biased by the experience of the researcher. The methodology can be summarized in the following major steps:

- Compiling documentation and resources. The document artifacts to be gathered include install, configuration, user guides, licensing schemes, and other relevant documents for each SIEM product.
- Forming an evaluation matrix for each testable aspect of the tools. This includes ease of use, installation, configurations functionality, performance, resource management, met requirements and cost.
- Create several virtual machines, one for each SIEM that will be testes and an attacker VM that will perform cyber-attacks. Install tools and run attacks against them. Produce the report based on results and use cases.

Tools and Use Cases

Test Environment Resources Used			
1 Laptop – HP Envy			
Number of CPUs	4 CPUs	RAM Memory	8 GB
CPU Speed	2.00 GHz	Storage	1 TB

SIEM Tools	Use Cases
Splunk	Regular User (Home Computer)
Prelude	Small Business (Small Store)
Elastic Stack / Wazuh	Large Company (Manufacturer)
OSSIM	Military (Missile Defense)

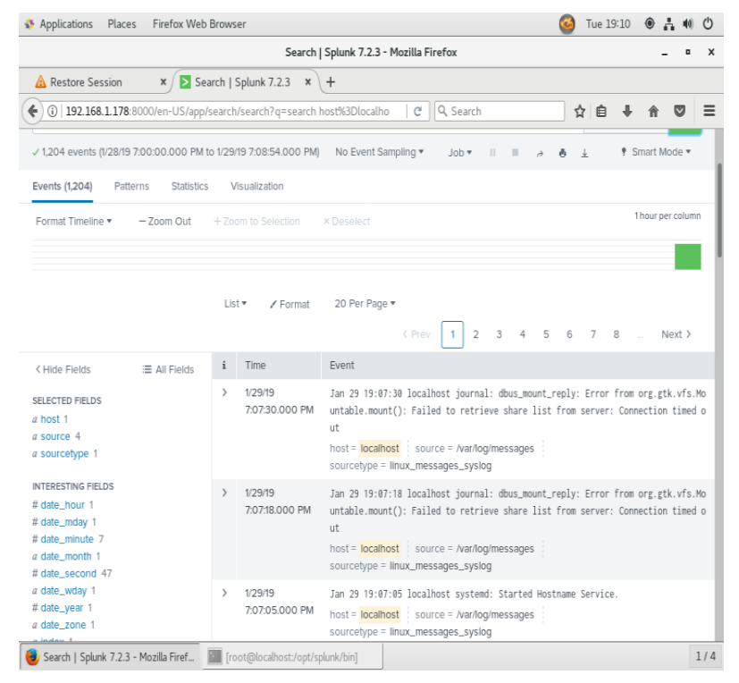
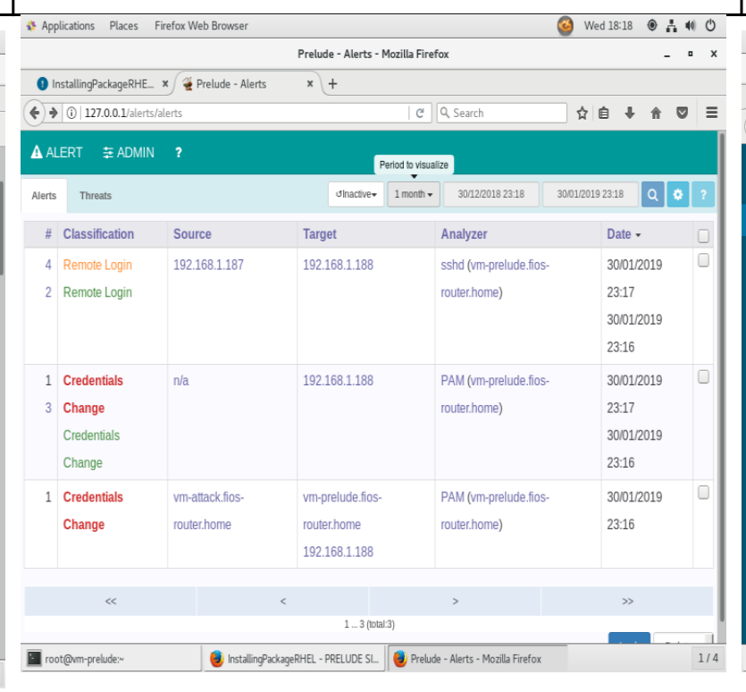
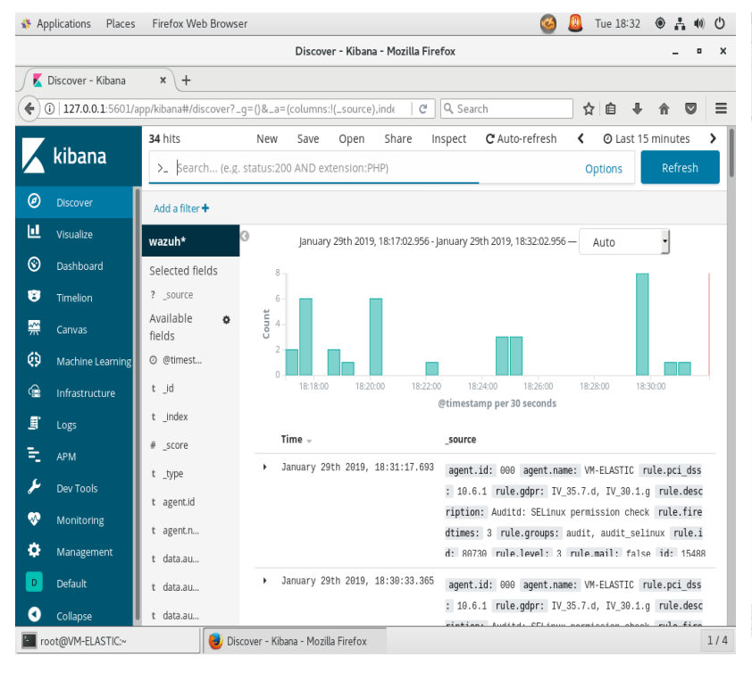
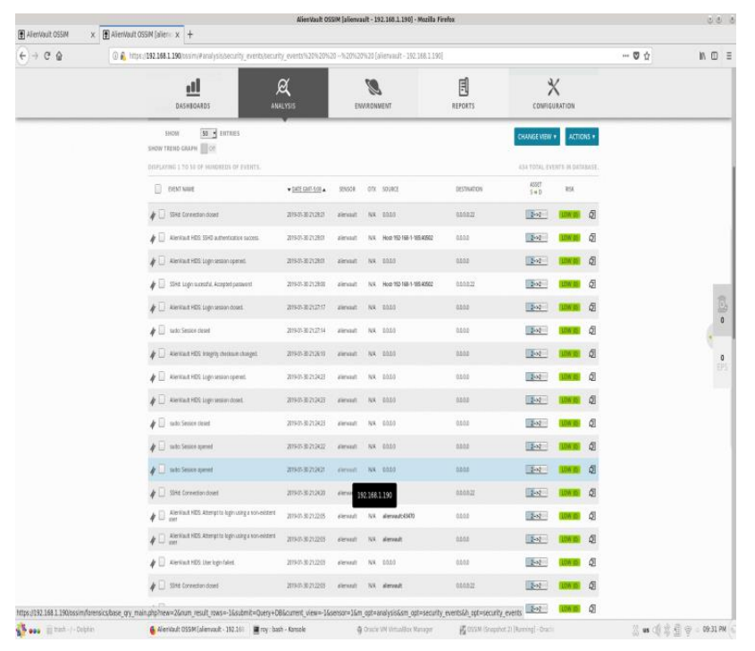
Results Metrics

AREA	METRIC	TOOLS / RESULTS			
		SPLUNK	PRELUDE	ELASTIC/WAZUH	OSSIM
COST FACTORS	DOES TEST VERSION HAVE ALL FEATURES AND SERVICES	NO	NO	YES	NO
	IS TEST VERSION DEPLOYABLE AS A SOLUTION	YES VERY LIMITED	YES	YES	NO 14 DAY TRIAL
	CAVEATS TO USING TEST VERSION	CAP ON DATA 500 MB	OTHER FEATURES NOT ENABLED	N/A	NOT ALL FEATURES ENABLED, LIMITED TRIAL
	LICENSING SCHEME	CHARGED DAILY BASED ON CAP DATA AMOUNT INGESTED BY SIEM. THE MORE DATA DESIRED THE CEAPER THE PRICE.	CHARGED BY EACH DEVICE CONNECTED TO THE OSSIM SERVER	FREE	FIXED PER INSTANCE, MONTHLY PAYMENTS START AT 1095
	GENERAL COST BASED ON LICENSING	50 PER 100GB DAILY	N/A FREE	FREE	1095 BASIC MO
	RENEWAL OF LICENSING	CAN BE PERPETUAL OR FIXED ON TERMS	N/A FREE	N/A	N/A
	ARE SECURITY PATCHES AND BUG FIXES SUPPORT INCLUDED IN LICENSING DEAL	YES	YES ON PAID, NO ON FREE	SOME	YES
	ARE THERE ADDITIONAL COSTS RELATED TO AQQUISITION	N/A	NO	N/A	N/A
	SUPPORT	THERE ARE PREMIUM SUPPORT LICENSING FOR ADDITIONAL SERVICES	THERE ARE PREMIUM SUPPORT LICENSING FOR ADDITIONAL SERVICES	THERE ARE PREMIUM SUPPORT LICENSING FOR ADDITIONAL SERVICES	THERE ARE PREMIUM SUPPORT LICENSING FOR ADDITIONAL SERVICES PRICE GOES UP TO 2600
RESOURCE FACTORS EXPECTED	NUMBER OF CPUS	2	N/A	N/A	N/A
	NUMBER OF CORES PER CPU	6	N/A	2	4
	CPU SPEED	2 Ghz	N/A	N/A	N/A
	RAM MEMORY	12 GB	N/A	8 GB	4 GB
	FREE HDD SPACE	5 GB	N/A	N/A	500 GB
	STORAGE	N/A	N/A	N/A	N/A
RESOURCE FACTORS ACTUALLY USED	NUMBER OF CPUS	2 CPU	2 CPU	2 CPU	2 CPU
	NUMBER OF CORES PER CPU	N/A	N/A	N/A	N/A
	CPU SPEED	N/A	N/A	N/A	N/A
	RAM MEMORY	2 GB	2 GB	4 GB	6 GB
	FREE HDD SPACE	4 GB	4.5 GB	5 GB	8.5 GB
	STORAGE	20 GB	20 GB	20 GB	30 GB
FEATURES FULLY LICENSED TOOLS	SECURITY	YES	YES	YES	YES
	CENTRALIZATION	YES	YES	YES	YES
	LOG MANAGEMENT	YES	YES	YES	YES
	DETECTION	YES	YES	YES	YES
	NORMALIZATION	YES	YES	YES	YES
	CORRELATION	YES	YES	YES	YES
	AGGREGATION	YES	YES	YES	YES
	ALERTING	YES	YES	YES	YES
	DATA VISUALIZATION	YES	YES	YES	YES
	METRICS	YES	YES	YES	YES
	REPORTING	YES	YES	YES	YES
	MONITORING	YES	NO	YES	YES
	MACHINE LEARNING	YES	NO	YES	NO
	THREAT INTELLIGENCE	NO	NO	NO	YES
FEATURES TRIAL VERSION TOOLS	SECURITY	YES	YES	YES	YES
	CENTRALIZATION	YES	YES	YES	YES
	LOG MANAGEMENT	YES	YES	YES	YES
	DETECTION	YES	YES	YES	YES
	NORMALIZATION	YES	YES	YES	YES
	CORRELATION	YES	YES	YES	YES
	AGGREGATION	YES	YES	YES	YES
	ALERTING	YES	NO	YES	NO
	DATA VISUALIZATION	YES	NO	YES	NO
	METRICS	YES	YES	YES	YES
	REPORTING	YES	NO	YES	YES
	MONITORING	YES	NO	YES	NO
	MACHINE LEARNING	YES	NO	YES	NO
	THREAT INTELLIGENCE	NO	NO	NO	YES
STANDARDS	PAYMENT CARD INDUSTRY DATA SECURITY STANDARDS (PCI DSS)	YES	YES	NO	YES
	INTERNATIONAL ORGANIZATION FOR STANDARDIZATION 27001 (ISO 27001)	NO	YES	NO	YES
	GENERAL DATA PROTECTION REGULATION (GDPR)	YES	NO	YES	NO
	HEALTH INSURANCE PORTABILITY ACT AND ACCOUNTABILITY ACT (HIPAA)	YES	NO	NO	YES
	INTTRUSION DETECTION MESSAGE EXCHANGE FORMAT (IDMEF)	NO	YES	NO	NO
	NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY CYBER SECURITY FRAMEWORK (NIST CSF)	YES	YES	NO	YES
DEPLOYABILITY	ACQUISITION COMPLEXITY STEPS	2 STEPS	2 STEPS	2 STEPS	2 STEPS
	AQQUISITION METHODOLOGY	SIGN UP AND DOWNLOAD	RPM YUM INSTALL	RPM YUM INSTALL	SIGN UP AND DOWNLOAD
	INSTALLATION COMPLEXITY STEPS	4 STEPS	22 STEPS	24 STEPS	4 STEPS
	INSTALLATION COMPLEXITY UNDERSTANDING	VERY EASY	EASY/STANDARD	EASY	VERY EASY
	INSTALLATION TIME	30 MINUTES	60 MINUTES	75 MINUTES	120 MINUTES
	CONFIGURATION COMPLEXITY STEPS	8 STEPS	N/A	N/A	5 STEPS
	CONFIGURATION COMPLEXITY UNDERSTANDING	VERY EASY	N/A	N/A	VERY EASY
USAGE	EASE OF ACCESS	1 TO 3 STEPS	1 TO 3 STEPS	1 TO 3 STEPS	1 TO 3 STEPS
	EASE OF TRAVERSAL	3 TO 5 STEPS	1 TO 3 STEPS	1 TO 3 STEPS	1 TO 3 STEPS
	VISUALY PLEASING	OK	GOOD	GOOD	GREAT
	UNDERSTANDABLE INTERFACE	OK	GREAT	GOOD	GOOD
FUNCTIONALITY	FAILED SSH ATTEMPT REGULAR USER	YES	YES	YES	N/A
	SUCESSFUL SSH ATTEMPT REGULAR USER	YES	YES	YES	N/A
	FAILED ROOT ESCALATION	YES	YES	YES	N/A
	SUCCESFUL SSH ATTEMPT ROOT USER	YES	YES	YES	YES
PERFORMANCE	FAILED SSH ATTEMPT REGULAR USER	5 SECONDS	5 SECONDS	8 SECONDS	N/A
	SUCESSFUL SSH ATTEMPT REGULAR USER	2 SECONDS	1 SECOND	<1 SECOND	N/A
	FAILED ROOT ESCALATION	7 SECONDS	1 SECOND	2 SECONDS	N/A
	SUCCESFUL SSH ATTEMPT ROOT USER	<1 SECOND	<1 SECOND	1 SECOND	2 SECONDS

Results Discussion

In terms of cost, the cheapest solution for a fully featured SIEM is Elastic. Prelude has a free version but it lacks several alerting and visualization features. The other tools have licensing fees that can rack up thousands of dollars per instance per month. Hardware resources are varied, documentation does not specify resources mostly. In practice the tool that requires the least amount of memory are Splunk and Prelude, by a huge margin. In terms of processors Splunk requires the least. Also it has the least mount of dedicated storage. All tools feature all required features to be considered a SIEM. Elastic and Splunk also contain machine learning modules. The easiest tool to install, configure and deploy is OSSIM. It only needs a root password and ip address and letting it run. Still the quickest one is Splunk. Using the tools themselves can be a little difficult, but the easiest experience and logical placement of items is with Prelude. Yet the most visually attractive tool is OSSIM. All tools were able to "alert" based on the performed tests. They are all very quick to respond, averaging mostly in less than 3 seconds per notification. The quickest to capture all events was Prelude.

All four use cases rely on different needs and requirements. The regular user is expected to have low resources in hardware and money, and only one computer. The user has no need for fancy features or services. The best tool for this user is either Prelude (free version) or Elastic. The small mom and pop shop have PCI DSS requirements since they handle credit card operations. We take them not as tech savvy so a hard to understand tool to use and deploy is not recommended. Hey could fork up some cash, but it is likely they don't have it. If they can pay OSSIM is their best bet, otherwise pick Elastic. The large manufacturing company has hundreds of devices in different networks, which will require several instances. A license that is based on device or data caps is a bad idea as it could costs hundreds of thousand of dollars. They are expected to have a significant amount of money so they can afford good hardware, a license and perhaps pay for some technical services. They should go with OSSIM, a flat rate per instance and capable running on good software. Finally a missile defense program. They have vast quantities of funding available, which helps with procuring hardware, license and premium services. Since their mission is one of life or death they need a tool that is most secure and have on the clock support. Splunk would be the best choice, also taking into account that tool is very popular on the military community. OSSIM is a close second, specially with their Threat Intelligence feature.

Splunk	Prelude	Elastic	OSSIM
			

Conclusion

A properly configured SIEM will capture a great deal of cyber events. Not only network, attacks, it can help with detecting malware, unwanted processes, corrupted files and so on. It I sproven that by having the tool instantiated one can look in a central place all of these events and could possibly act on them. By having a testing framework to test its functionality and performance, and having quantifiable or qualitative metrics regarding questions needed to comply with the users requirements; funds, time and human resources are reduced in order to choose a SIEM. Every tool works, and is even better for each specific case. By the data Prelude and OSSIM are concluded to ne the better tools overall.

References

[1]Miller, D., Harris, S., Harper, A., Van Dyke, S., Blask, C.: Security Information and Event Management (SIEM) Implementation. Mc Graw Hill (2010)

[2] Reynoso Vásquez, V. K. (2009). Events Centralization and Correlation at a Finance Entity.

[3] Kotenko, I., & Chechulin, A. (2012). Attack modeling and security evaluation in SIEM systems. International Transactions on Systems Science and Applications, 8, 129-147.

[4] Kent, K., & Souppaya, M. (2006). Guide to computer security log management. NIST special publication, 92.

[5] Hubbard, D, (April 28 – May 3, 2013). How to Measure Anything: An Introduction from the Author, Webinar based on authors book How to Measure Anything, Retrieved from https://www.youtube.com/watch?v=w4fHGTsZZD8

[6] Rieke, R., Coppolino, L., Hutchison, A., Prieto, E., & Gaber, C. (2012, October). Security and reliability requirements for advanced security event management. In International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security (pp. 171-180). Springer, Berlin, Heidelberg.